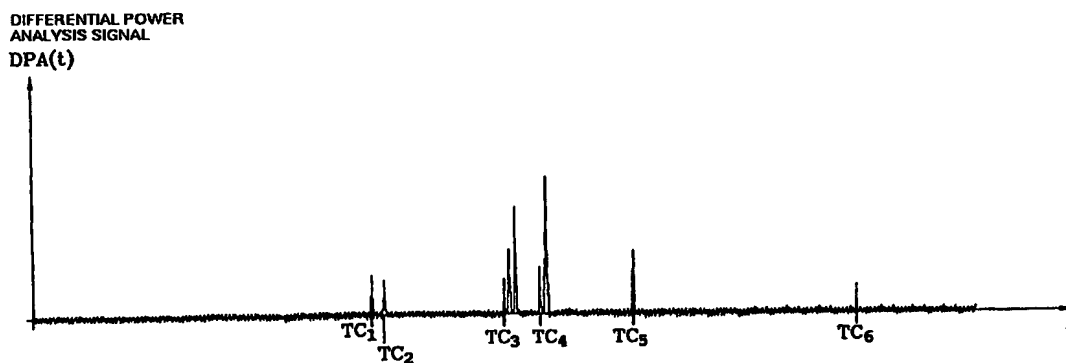


**PCT**ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE  
Bureau international

L-16

DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

<b>(51) Classification internationale des brevets <sup>7</sup> :</b> <b>H04L 9/06</b>	<b>A1</b>	<b>(11) Numéro de publication internationale:</b> <b>WO 00/24156</b> <b>(43) Date de publication internationale:</b> 27 avril 2000 (27.04.00)
<b>(21) Numéro de la demande internationale:</b> PCT/FR99/02199 <b>(22) Date de dépôt international:</b> 15 septembre 1999 (15.09.99)  <b>(30) Données relatives à la priorité:</b> 98/12990                      16 octobre 1998 (16.10.98)                      FR  <b>(71) Déposant (pour tous les Etats désignés sauf US):</b> GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).  <b>(71)(72) Déposants et inventeurs:</b> CLAVIER, Christophe [FR/FR]; 5, rue de la République, F-13420 Gémenos (FR). BENOIT, Olivier [FR/FR]; La Treille d'Azur, Bâtiment D, Avenue du 19 Mars 1962, F-13400 Aubagne (FR).  <b>(74) Mandataire:</b> NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).		<b>(81) Etats désignés:</b> AU, CA, CN, IN, JP, MX, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Publiée</b> <i>Avec rapport de recherche internationale.</i>

**(54) Title:** COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM**(54) Titre:** PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE**(57) Abstract**

The invention concerns a countermeasure method in an electronic component using a secret key K cryptographic algorithm with sixteen computing cycles to supply an encrypted message (C) from an input message (M), each cycle using first means TC<sub>0</sub> to supply an output information from an input information, Said method consists in applying by selection a sequence with the first means or another sequence with other means TC<sub>1</sub>, TC<sub>2</sub> to a group G1 comprising the first three cycles at least and another group G4 comprising the last three cycles at least. Whatever the sequence, the output result of the last cycle of each group is the same for the same input message (M).

(57) Abrégé

Dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (K) à seize tours de calcul pour fournir un message chiffré (C) à partir d'un message d'entrée (M), chaque tour utilisant des premiers moyens TC<sub>0</sub> pour fournir une donnée de sortie à partir d'une donnée d'entrée, on applique au choix une séquence avec les premiers moyens ou une autre séquence avec d'autres moyens TC<sub>1</sub>, TC<sub>2</sub> à un groupe G1 comprenant les trois premiers tours au moins et un autre groupe G4 comprenant les trois derniers tours au moins. Quelle que soit la séquence, le résultat en sortie du dernier tour de chaque groupe est le même pour un même message d'entrée (M).

**UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Bésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun	KR	République de Corée	PL	Pologne		
CN	Chine	KZ	Kazakstan	PT	Portugal		
CU	Cuba	LC	Sainte-Lucie	RO	Roumanie		
CZ	République tchèque	LI	Liechtenstein	RU	Fédération de Russie		
DE	Allemagne	LK	Sri Lanka	SD	Soudan		
DK	Danemark	LR	Libéria	SE	Suède		
EE	Estonie			SG	Singapour		

PROCÉDÉ DE CONTRE-MESURE DANS UN COMPOSANT  
ÉLECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE  
CRYPTOGRAPHIE A CLÉ SECRÈTE

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé secrète. Ils sont utilisés dans des applications où l'accès à  
5 des services ou à des données est sévèrement contrôlé. Ils ont une architecture formée autour d'un microprocesseur et de mémoires, dont une mémoire programme qui contient la clé secrète.

Ces composants sont notamment utilisés dans les  
10 cartes à puce, pour certaines applications de celles-ci. Ce sont par exemple des applications d'accès à certaines banques de données, des applications bancaires, des applications de télépéage, par exemple pour la télévision, la distribution d'essence ou encore  
15 le passage de péages d'autoroutes.

Ces composants ou ces cartes mettent donc en oeuvre un algorithme de cryptographie à clé secrète, dont le plus connu est l'algorithme DES (pour *Data Encryption Standard* dans la littérature anglo-saxonne). D'autres  
20 algorithmes à clé secrète existent, comme l'algorithme RC5 ou encore l'algorithme COMP128. Cette liste n'est bien sûr pas exhaustive.

De manière générale et succincte, ces algorithmes ont pour fonction de calculer un message chiffré à  
25 partir d'un message appliqué en entrée (à la carte) par un système hôte (serveur, distributeur bancaire...) et de la clé secrète contenue dans la carte, et de fournir en retour au système hôte ce message chiffré, ce qui permet par exemple au système hôte d'authentifier le  
30 composant ou la carte, d'échanger des données...

Or il est apparu que ces composants ou ces cartes sont vulnérables à des attaques consistant en une analyse différentielle de consommation en courant et qui permettent à des tiers mal intentionnés de trouver la clé secrète. Ces attaques sont appelées attaques DPA, acronyme anglo-saxon pour *Differential Power Analysis*.

Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

Notamment, une instruction du microprocesseur manipulant un bit de donnée génère deux profils de courant différents selon que ce bit vaut "1" ou "0". Typiquement, si l'instruction manipule un "0", on a à cet instant d'exécution une première amplitude du courant consommé et si l'instruction manipule un "1", on a une deuxième amplitude du courant consommé, différente de la première.

Les caractéristiques des algorithmes de cryptographie sont connues : calculs effectués, paramètres utilisés. La seule inconnue est la clé secrète contenue en mémoire programme. Celle-ci ne peut être déduite de la seule connaissance du message appliqué en entrée et du message chiffré fourni en retour.

Cependant, dans un algorithme de cryptographie, certaines données calculées dépendent seulement du message appliqué en clair en entrée de la carte et de la clé secrète contenue dans la carte. D'autres données calculées dans l'algorithme peuvent aussi être recalculées seulement à partir du message chiffré (généralement fourni en clair en sortie de la carte vers le système hôte) et de la clé secrète contenue dans la carte. Plus précisément, chaque bit de ces données particulières peut être déterminé à partir du

message d'entrée ou de sortie, et d'un nombre limité de bits particuliers de la clé.

Ainsi, à chaque bit d'une donnée particulière, correspond une sous-clé formée par un groupe  
5 particulier de bits de la clé.

Les bits de ces données particulières qui peuvent être prédites sont appelés dans la suite, bits cibles.

L'idée de base de l'attaque DPA est ainsi d'utiliser la différence du profil de consommation en  
10 courant d'une instruction selon qu'elle manipule un "1" ou un "0" et la possibilité de calculer un bit cible par les instructions de l'algorithme à partir d'un message connu d'entrée ou de sortie et d'une hypothèse sur la sous-clé correspondante.

15 Le principe de l'attaque DPA est donc de tester une hypothèse de sous-clé donnée, en appliquant sur un grand nombre de courbes de mesure en courant, chacune relative à un message d'entrée connu de l'attaquant, une fonction booléenne de sélection, fonction de  
20 l'hypothèse de sous-clé, et définie pour chaque courbe par la valeur prédite pour un bit cible.

En faisant une hypothèse sur la sous-clé concernée, on est en effet capable de prédire la valeur "0" ou "1" que va prendre ce bit cible pour un message d'entrée ou  
25 de sortie donné.

On peut alors appliquer comme fonction booléenne de sélection, la valeur prédite "0" ou "1" par le bit cible pour l'hypothèse de sous-clé considérée, pour trier ces courbes en deux paquets : un premier paquet  
30 regroupe les courbes qui ont vu la manipulation du bit cible à "0" et un deuxième paquet regroupe les courbes qui ont vu la manipulation du bit cible à "1" selon l'hypothèse de sous-clé. En faisant la moyenne de consommation en courant dans chaque paquet, on obtient  
35 une courbe de consommation moyenne  $M0(t)$  pour le

premier paquet et une courbe de consommation moyenne  $M_1(t)$  pour le deuxième paquet.

Si l'hypothèse de sous-clé est juste, le premier paquet regroupe réellement toutes les courbes parmi les  
 5 N courbes qui ont vu la manipulation du bit cible à "0" et le deuxième paquet regroupe réellement toutes les courbes parmi les N courbes qui ont vu la manipulation du bit cible à "1". La courbe moyenne de consommation  $M_0(t)$  du premier paquet aura alors une consommation  
 10 moyenne partout sauf aux moments de l'exécution des instructions critiques, avec un profil de consommation en courant caractéristique de la manipulation du bit cible à "0" ( $\text{profil}_0$ ). En d'autres termes, pour toutes ces courbes tous les bits manipulés ont eu autant de  
 15 chances de valoir "0" que de valoir "1", sauf le bit cible qui a toujours eu la valeur "0". Ce qui peut s'écrire :

$$M_0(t) = [(\text{profil}_0 + \text{profil}_1)/2]_{t \neq t_{ci}} + [\text{profil}_0]_{t_{ci}} \text{ soit}$$

$$M_0(t) = [V_{m_t}]_{t \neq t_{ci}} + [\text{profil}_0]_{t_{ci}}$$

20 où  $t_{ci}$  représente les instants critiques, auxquels une instruction critique a été exécutée.

De même, la courbe moyenne de consommation  $M_1(t)$  du deuxième paquet correspond à une consommation moyenne partout sauf aux moments de l'exécution des  
 25 instructions critiques, avec un profil de consommation en courant caractéristique de la manipulation du bit cible à "1" ( $\text{profil}_1$ ). On peut écrire :

$$M_1(t) = [(\text{profil}_0 + \text{profil}_1)/2]_{t \neq t_{ci}} + [\text{profil}_1]_{t_{ci}} \text{ soit}$$

$$M_1(t) = [V_{m_t}]_{t \neq t_{ci}} + [\text{profil}_1]_{t_{ci}}$$

30 On a vu que les deux profils  $\text{profil}_0$  et  $\text{profil}_1$  ne sont pas égaux. La différence des courbes  $M_0(t)$  et  $M_1(t)$  donne alors un signal  $DPA(t)$  dont l'amplitude est égale à  $\text{profil}_0 - \text{profil}_1$  aux instants critiques  $t_{ci}$  d'exécution des instructions critiques manipulant ce  
 35 bit, c'est à dire, dans l'exemple représenté sur la figure 1, aux endroits  $tc_0$  à  $tc_6$  et dont l'amplitude

est à peu près égale à zéro en dehors des instants critiques.

Si l'hypothèse de sous-clé est fausse, le tri ne correspond pas à la réalité. Statistiquement, il y a alors dans chaque paquet, autant de courbes ayant vu réellement la manipulation du bit cible à "0" que de courbes ayant vu la manipulation du bit cible à "1". La courbe moyenne résultante  $M0(t)$  se situe alors autour d'une valeur moyenne donnée par  $(profil_0 + profil_1)/2 = V_m$ , car pour chacune des courbes, tous les bits manipulés, y compris le bit cible ont autant de chances de valoir "0" que de valoir "1".

Le même raisonnement sur le deuxième paquet conduit à une courbe moyenne de consommation en courant  $M1(t)$  dont l'amplitude se situe autour d'une valeur moyenne donnée par  $(profil_0 + profil_1)/2 = V_m$ .

Le signal  $DPA(t)$  fourni par la différence  $M0(t) - M1(t)$  est dans ce cas sensiblement égal à zéro. Le signal  $DPA(t)$  dans le cas d'une hypothèse de sous-clé fausse est représenté sur la figure 2.

Ainsi l'attaque DPA exploite la différence du profil de consommation en courant pendant l'exécution d'une instruction suivant la valeur du bit manipulé, pour effectuer un tri de courbes de consommation en courant selon une fonction de sélection booléenne pour une hypothèse de sous-clé donnée. En effectuant une analyse différentielle de la consommation moyenne en courant entre les deux paquets de courbes obtenus, on obtient un signal d'information  $DPA(t)$ .

Le déroulement d'une attaque DPA consiste alors globalement:

a- à tirer N messages aléatoires (par exemple N égal 1000);

b- à faire exécuter l'algorithme par la carte pour chacun des N messages aléatoires, en relevant la courbe

de consommation en courant à chaque fois (mesurée sur la borne d'alimentation du composant);

c- à faire une hypothèse sur une sous-clé;

5 d- à prédire, pour chacun des messages aléatoires, la valeur prise par un des bits cibles dont la valeur ne dépend que des bits du message (d'entrée ou de sortie) et de la sous-clé prise en hypothèse, pour obtenir la fonction de sélection booléenne;

10 e- à trier les courbes selon cette fonction de sélection booléenne (c'est à dire selon la valeur "0" ou "1" prédite pour ce bit cible pour chaque courbe sous l'hypothèse de sous-clé);

f- à calculer dans chaque paquet la courbe résultante de consommation moyenne en courant;

15 g- à effectuer la différence de ces courbes moyennes, pour obtenir le signal DPA(t).

20 Si l'hypothèse sur la sous-clé est juste, la fonction de sélection booléenne est juste et les courbes du premier paquet correspondent réellement aux courbes pour lesquelles le message appliqué en entrée ou en sortie a donné un bit cible à "0" dans la carte et les courbes du deuxième paquet correspondent réellement aux courbes pour lesquelles le message appliqué en entrée ou en sortie a donné un bit cible à  
25 "1" dans la carte.

On est dans le cas de la figure 1 : le signal DPA(t) n'est donc pas nul aux instants  $tc_0$  à  $tc_6$  correspondant à l'exécution des instructions critiques (celles qui manipulent le bit cible). Il suffit qu'il y  
30 ait au moins un instant critique dans la période d'acquisition.

On notera que l'attaquant n'a pas besoin de connaître avec précision les instants critiques.

35 Si l'hypothèse de sous-clé n'est pas juste, le tri ne correspond pas à la réalité et on a alors dans chaque paquet autant de courbes correspondant en

réalité à un bit cible à "0" que de courbes correspondant à un bit cible à "1". Le signal DPA(t) est sensiblement nul partout (cas représenté à la figure 2). Il faut retourner à l'étape c- et faire une

5 nouvelle hypothèse sur la sous-clé.

Si l'hypothèse s'avère juste, on peut passer à l'évaluation d'autres sous-clés, jusqu'à avoir reconstitué la clé au maximum. Par exemple, avec un algorithme DES, on utilise une clé de 64 bits, dont

10 seulement 56 bits utiles. Avec une attaque DPA, on est capable de reconstituer au moins 48 bits des 56 bits utiles.

La présente invention a pour but de mettre en oeuvre dans un composant électronique, un procédé de contre-mesure qui entraîne un signal DPA(t) nul, même

15 dans le cas où l'hypothèse de sous-clé est juste.

De cette façon, rien ne permet de distinguer le cas de l'hypothèse de sous-clé juste des cas d'hypothèses de sous-clé fausses. Par cette contre-mesure, le

20 composant électronique est paré contre les attaques DPA.

Selon l'invention, le procédé de contre-mesure permet de rendre imprédictibles les bits cibles, c'est à dire les données manipulées par des instructions

25 critiques.

En effet, du fait de la contre-mesure, pour chaque message appliqué en entrée, un bit cible manipulé par une instruction critique prend la valeur 0 ou 1 avec une égale probabilité. Dans chaque paquet de courbes

30 que fera l'attaquant sous une hypothèse de sous-clé donnée, au moyen de la fonction de sélection booléenne qu'il aura calculée, on aura autant de courbes ayant réellement manipulé un bit cible "0" que de courbes ayant réellement manipulé un bit cible à "1". Le signal

35 DPA(t) sera toujours nul, que l'hypothèse de sous-clé soit juste ou non.

Dans l'invention, on s'intéresse plus particulièrement à l'algorithme de cryptographie DES.

Un tel algorithme comprend seize tours de calcul identiques.

5 Dans un tel algorithme, on a pu mettre en évidence que les données prédictibles par un attaquant se situent au premier tour et au dernier tour, et que les instructions critiques au sens de l'attaque DPA se situent dans les trois premiers tours et les trois  
10 derniers tours.

Dans l'invention, on a plus particulièrement cherché un moyen de rendre imprédictibles les données manipulées par ces instructions critiques des trois premiers et trois derniers tours, tout en obtenant le  
15 bon message chiffré en sortie.

Un but de l'invention est donc de rendre imprédictibles les données manipulées par les instructions critiques, tout en obtenant le bon résultat final (message chiffré C).

20 Une solution à ces différents problèmes techniques a été trouvée dans la formation d'un groupe (G1) comprenant au moins les trois premiers tours et d'un autre groupe (G4) comprenant au moins les trois derniers tours, et dans l'utilisation dans ces groupes  
25 de moyens pour rendre imprédictibles les données manipulées par les instructions critiques contenues dans ces tours.

Selon l'invention, les résultats en sortie de chaque groupe sont justes.

30 Telle que caractérisée, l'invention concerne donc un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète pour calculer un message  
35 chiffré à partir d'un message d'entrée, la mise en oeuvre de l'algorithme comprenant seize tours de

calcul, chaque tour utilisant des premiers moyens pour  
fournir une donnée de sortie à partir d'une donnée  
d'entrée, la donnée de sortie et/ou des données  
dérivées étant manipulées par des instructions  
5 critiques dans les trois premiers et les trois derniers  
tours. Selon l'invention, on forme un groupe comprenant  
les trois premiers tours au moins et un autre groupe  
comprenant les trois derniers tours au moins, et on  
associe à chacun de ces groupes une première séquence  
10 utilisant les premiers moyens dans chaque tour et une  
deuxième séquence utilisant d'autres moyens dans  
certains tours au moins, les dites première et deuxième  
séquences étant telles qu'elles fournissent un même  
résultat en sortie du dernier tour de chaque groupe  
15 pour un même message d'entrée donné, le choix de la  
séquence à exécuter dans les groupes concernés étant  
fonction d'une loi statistique de probabilité un demi,  
pour rendre imprédictibles toutes les données  
manipulées par les dites instructions critiques.

20 Dans un mode de réalisation, on forme quatre  
groupes de quatre tours consécutifs chacun.

Dans un autre mode de réalisation, on forme deux  
groupes comprenant respectivement les trois premiers et  
les trois derniers tours.

25 D'autres caractéristiques et avantages de  
l'invention sont détaillés dans la description suivante  
faite à titre indicatif et nullement limitatif et en  
référence aux dessins annexés, dans lesquels :

30 - les figures 1 et 2 déjà décrites représentent le  
signal  $DPA(t)$  que l'on peut obtenir en fonction d'une  
hypothèse sur une sous-clé de la clé secrète  $K$ , selon  
une attaque DPA;

35 - les figures 3 et 4 sont des organigrammes  
représentant les premiers tours et les derniers tours  
de l'algorithme DES;

- la figure 5 est un schéma-bloc de l'opération SBOX utilisée dans l'algorithme DES;

5       - la figure 6 montre un exemple de table de constante élémentaire à une entrée et une sortie utilisée dans l'opération SBOX;

      - la figure 7 représente un premier exemple d'organigramme d'exécution du DES avec un procédé de contre-mesure selon l'invention;

10       - la figure 8 est un organigramme des premiers tours du DES selon une deuxième séquence du procédé de contre-mesure selon le premier exemple représenté à la figure 7;

15       - Les figures 9 et 10 représentent respectivement une deuxième et une troisième tables de constantes élémentaires utilisées dans l'invention;

      - la figure 11 représente un deuxième exemple d'organigramme d'exécution du DES avec un procédé de contre mesure selon l'invention;

20       - les figures 12 et 13 sont des organigrammes des premiers tours de DES respectivement selon la deuxième séquence et la première séquence du procédé de contre-mesure selon le deuxième exemple représenté à la figure 11;

25       - les figures 14 et 15 sont des organigrammes relatifs à un troisième mode d'application du procédé de contre-mesure selon l'invention;

      - la figure 16 représente une troisième table de constantes élémentaire utilisée dans ce quatrième mode d'application de l'invention;

30       - la figure 17 représente un organigramme d'exécution du DES selon une variante du troisième mode d'application du procédé de contre-mesure selon l'invention; et

35       - la figure 18 représente un schéma-bloc simplifié d'une carte à puce comportant un composant électronique

dans lequel le procédé de contre-mesure selon l'invention est mis en oeuvre.

5 L'algorithme cryptographique à clé secrète DES (dans la suite on parlera plus simplement du DES ou de l'algorithme DES) comporte 16 tours de calcul, notés T1 à T16, comme représenté sur les figures 3 et 4.

10 Le DES débute par une permutation initiale IP sur le message d'entrée M (figure 3). Le message d'entrée M est un mot f de 64 bits. Après permutation, on obtient un mot e de 64 bits, que l'on coupe en deux pour former les paramètres d'entrée L0 et R0 du premier tour (T1). L0 est un mot d de 32 bits contenant les 32 bits de poids forts du mot e. R0 est un mot h de 32 bits  
15 contenant les 32 bits de poids faibles du mot e.

La clé secrète K, qui est un mot q de 64 bits subit elle-même une permutation et une compression pour fournir un mot r de 56 bits.

20 Le premier tour comprend une opération EXP PERM sur le paramètre R0, consistant en une expansion et une permutation, pour fournir en sortie un mot l de 48 bits.

25 Ce mot l est combiné à un paramètre K1, dans une opération de type OU EXCLUSIF notée XOR, pour fournir un mot b de 48 bits. Le paramètre K1 qui est un mot m de 48 bits est obtenu du mot r par un décalage d'une position (opération notée SHIFT sur les figures 3 et 4) suivi d'une permutation et d'une compression (opération notée COMP PERM).

30 Le mot b est appliqué à une opération notée SBOX, en sortie de laquelle on obtient un mot a de 32 bits. Cette opération particulière sera expliquée plus en détail en relation avec les figures 5 et 6.

35 Le mot a subit une permutation P PERM, donnant en sortie le mot c de 32 bits.

Ce mot c est combiné au paramètre d'entrée L0 du premier tour T1, dans une opération logique de type OU EXCLUSIF, notée XOR, qui fournit en sortie le mot g de 32 bits.

5        Le mot h (=R0) du premier tour fournit le paramètre d'entrée L1 du tour suivant (T2) et le mot g du premier tour fournit le paramètre d'entrée R1 du tour suivant. Le mot p du premier tour fournit l'entrée r du tour suivant.

10       Les autres tours T2 à T16 se déroulent de façon similaire, excepté en ce qui concerne l'opération de décalage SHIFT qui se fait sur une ou deux positions selon les tours considérés.

15       Chaque tour Ti reçoit ainsi en entrée les paramètres Li-1, Ri-1 et r et fournit en sortie les paramètres Li et Ri et r pour le tour suivant Ti+1.

En fin d'algorithme DES (figure 4), le message chiffré est calculé à partir des paramètres L16 et R16 fournis par le dernier tour T16.

20       Ce calcul du message chiffré C comprend en pratique les opérations suivantes :

- formation d'un mot e' de 64 bits en inversant la position des mots L16 et R16, puis en les concaténant;
  - application de la permutation  $IP^{-1}$  inverse de celle de début de DES, pour obtenir le mot f' de 64 bits formant le message chiffré C.
- 25

L'opération SBOX est détaillée sur les figures 5 et 6. Elle comprend une table de constantes  $TC_0$  pour fournir une donnée de sortie a en fonction d'une donnée d'entrée b.

30

En pratique, cette table de constantes  $TC_0$  se présente sous la forme de huit tables de constantes élémentaires  $TC_{01}$  à  $TC_{08}$ , chacune recevant en entrée seulement 6 bits du mot b, pour fournir en sortie seulement 4 bits du mot a.

35

Ainsi, la table de constante élémentaire  $TC_01$  représentée sur la figure 6 reçoit comme donnée d'entrée, les bits  $b1$  à  $b6$  du mot  $b$  et fournit comme donnée de sortie les bits  $a1$  à  $a4$  du mot  $a$ .

5        En pratique ces huit tables de constantes élémentaires  $TC_01$  à  $TC_08$  sont mémorisées en mémoire programme du composant électronique.

10       Dans l'opération SBOX du premier tour  $T1$ , un bit particulier de la donnée  $a$  de sortie de la table de constante  $TC_0$  dépend de seulement 6 bits de la donnée  $b$  appliquée en entrée, c'est à dire de seulement 6 bits de la clé secrète  $K$  et du message d'entrée ( $M$ ).

15       Dans l'opération SBOX du dernier tour  $T16$ , un bit particulier de la donnée  $a$  de sortie de la table de constante  $TC_0$  peut être recalculé à partir de seulement 6 bits de la clé secrète  $K$  et du message chiffré ( $C$ ).

20       Or si on reprend le principe de l'attaque DPA, si on choisit comme bit cible un bit de la donnée de sortie  $a$ , il suffit de faire une hypothèse sur 6 bits de la clé  $K$ , pour prédire la valeur d'un bit cible pour un message d'entrée ( $M$ ) ou de sortie ( $C$ ) donné. En d'autres termes, pour le DES, il suffit de faire une hypothèse sur une sous-clé de 6 bits.

25       Dans une attaque DPA sur un tel algorithme pour un bit cible donné, on a donc à discriminer une hypothèse de sous-clé juste parmi 64 possibles.

30       Ainsi, en prenant seulement huit bits du mot  $a$  comme bits cibles, (un bit de sortie par table de constantes élémentaire  $TC_01$  à  $TC_08$ ), on peut découvrir jusqu'à  $6 \times 8 = 48$  bits de la clé secrète, en faisant des attaques DPA sur chacun de ces bits cibles.

      Dans le DES, on trouve donc des instructions critiques au sens des attaques DPA au début de l'algorithme et à la fin.

35       Au début de l'algorithme DES, les données qui peuvent être prédites à partir d'un message d'entrée  $M$

et d'une hypothèse de sous-clé, sont les données a et g calculées dans le premier tour (T1).

La donnée a du premier tour T1 (figure 3) est la donnée de sortie de l'opération SBOX du tour considéré.

5 La donnée g est calculée à partir de la donnée a, par permutation (P PERM) et opération OU EXCLUSIF avec le paramètre d'entrée L0.

En fait, la donnée c du premier tour, est une donnée dérivée de la donnée a du premier tour. La  
10 donnée dérivée c correspond à une simple permutation de bits de la donnée a.

La donnée l du deuxième tour est une donnée dérivée de la donnée g du premier tour, car elle correspond à une permutation des bits du mot g, certains bits du mot  
15 g étant en outre dupliqués.

Connaissant a et g, on peut aussi connaître ces données dérivées.

Les instructions critiques du début de l'algorithme sont les instructions critiques qui manipulent soit la  
20 donnée que l'on peut prédire, comme la donnée a du premier tour, soit une donnée dérivée.

Les instructions critiques manipulant la donnée a du premier tour T1 ou la donnée dérivée c sont ainsi les instructions de fin de l'opération SBOX, de  
25 l'opération P PERM et de début de l'opération XOR du premier tour T1.

Les instructions critiques manipulant la donnée g ou des données dérivées sont toutes les instructions de de fin d'opération XOR de fin du premier tour T1  
30 jusqu'aux instructions de début d'opération SBOX du deuxième tour T2, et de début de l'opération XOR en fin du troisième tour T3 ( $L2 = h(T2) = g(T1)$  ).

En fin d'algorithme DES, les données qui peuvent être prédites à partir d'un message chiffré C et d'une  
35 hypothèse de sous-clé, sont la donnée a du seizième

tour T16 et la donnée L15 égale au mot h du quatorzième tour T14.

Les instructions critiques manipulant la donnée a du seizième tour ou des données dérivées sont les  
5 instructions du seizième tour de fin d'opération SBOX, de l'opération de permutation P PERM et de début d'opération XOR.

Pour la donnée L15, les instructions critiques manipulant cette donnée ou des données dérivées sont  
10 toutes les instructions depuis les instructions de fin d'opération XOR du quatorzième tour T14, jusqu'aux instructions de début d'opération SBOX du quinzième tour T15, plus les instructions de début d'opération XOR du seizième tour T16.

15 Le procédé de contre-mesure selon l'invention appliqué à cet algorithme DES consiste à avoir, pour chaque instruction critique, autant de chances que l'instruction critique manipule une donnée que son complément. Ainsi, quel que soit le bit cible sur  
20 lequel l'attaque DPA peut être faite, on a autant de chances que les instructions critiques qui manipulent ce bit, manipulent un "1" ou un "0".

En pratique, ceci doit être vrai pour chacun des bits cibles potentiels : en d'autres termes,  
25 l'attaquant ayant le choix entre plusieurs attaques possibles, c'est à dire entre plusieurs fonctions de sélection booléenne possibles pour effectuer son tri de courbes, pour une hypothèse de sous-clé donnée, la mise en oeuvre du procédé de contre-mesure selon l'invention  
30 doit s'attacher à ce que les données manipulées par chacune des instructions critiques, prennent aléatoirement, une fois sur deux, une valeur ou son complément. En ce qui concerne l'application du procédé de contre-mesure selon l'invention à l'algorithme DES,  
35 il faut donc appliquer la contre-mesure aux instructions critiques de début de DES et aux

instructions critiques de fin de DES, pour être totalement protégé.

Dans le DES, toutes les données manipulées par des instructions critiques sont une donnée de sortie ou des données dérivées d'une donnée de sortie d'une opération SBOX.

En effet, en début de DES, les données qui peuvent être prédites sont les données a et g du premier tour T1. La donnée a est la donnée de sortie de l'opération SBOX du premier tour. La donnée g est calculée à partir de la donnée a, puisque  $g = P \text{ PERM}(a) \text{ XOR } L0$ . g est donc une donnée dérivée de la donnée de sortie a de l'opération SBOX du premier tour. Ainsi, toutes les données manipulées par les instructions critiques de début de DES découlent directement ou indirectement de la donnée de sortie a de l'opération SBOX du premier tour.

En ce qui concerne la fin de DES, les données qui peuvent être prédites sont la donnée a du seizième tour T16 et la donnée g du quatorzième tour T14, g étant égale à L15.

La donnée a est la donnée de sortie de l'opération SBOX du seizième tour T16.

Quant à la donnée L15, elle se calcule, dans l'exécution normale de l'algorithme DES, à partir de la donnée de sortie a de l'opération SBOX du quatorzième tour T14 :  $L15 = P \text{ PERM}(a) \text{ XOR } L14$ .

Si on rend imprédictibles les données de sortie a de ces opérations SBOX particulières, on rend aussi imprédictibles toutes les données dérivées : on rend donc imprédictibles toutes les données manipulées par les instructions critiques de l'algorithme DES. Si on considère que ces opérations SBOX constituent des premiers moyens pour fournir une donnée de sortie  $S=a$  à partir d'une donnée d'entrée  $E=b$ , le procédé de contre-mesure appliqué à l'algorithme DES consiste à utiliser

d'autres moyens pour rendre imprédictibles la donnée de sortie, en sorte que cette donnée de sortie et/ou des données dérivées manipulées par les instructions critiques soient toutes imprédictibles.

5            Selon l'invention, on forme un groupe formé des trois premiers tours au moins et un autre groupe formé des trois derniers tours au moins. Ces groupes contiennent donc tous les tours comprenant des instructions critiques.

10           On associe à ces deux groupes une première séquence utilisant les premiers moyens pour tous les tours et une deuxième séquence utilisant les autres moyens pour certains tours au moins.

15           Dans les autres tours qui ne sont pas dans ces groupes, on peut continuer à utiliser les premiers moyens.

L'utilisation de ces autres moyens est telle que le résultat en sortie, c'est à dire, le message chiffré reste juste.

20           Ces autres moyens peuvent comprendre plusieurs moyens différents. Ils sont tels qu'à l'une et/ou l'autre donnée parmi les données d'entrée et de sortie de premiers moyens, ils font correspondre la donnée complémentée.

25           Ainsi, considérant un grand nombre d'exécution, les groupes utiliseront en moyenne une fois sur deux la première séquence, qui est la séquence normale de l'algorithme, et une fois sur deux l'autre séquence. Les données manipulées par les instructions critiques  
30           dans ces groupes, correspondant à certains résultats intermédiaires, seront donc en moyenne complémentées une fois sur deux. Sur un grand nombre de courbes on aura donc statistiquement autant de chances qu'un bit cible donné soit à 1 ou à 0.

35           La figure 7 représente un premier mode de réalisation de l'invention.

Dans ce mode de réalisation, on répartit les seize tours de l'algorithme DES en quatre groupes G1 à G4 de quatre tours successifs. Le groupe G1 comprend ainsi les tours T1 à T4, le groupe G2, les tours T5 à T8, le groupe G3, les tours T9 à T12 et le groupe G4, les tours T13 à T16.

A chaque groupe, on associe deux séquences. Une première séquence SEQA consiste à utiliser les premiers moyens  $TC_0$  pour chaque tour. Une deuxième séquence SEQB consiste à utiliser d'autres moyens pour certains tours au moins.

Dans l'exemple représenté, ces autres moyens comprennent des deuxièmes moyens  $TC_2$  et des troisièmes moyens  $TC_1$ .

Les deuxièmes moyens  $TC_2$  sont utilisés dans le deuxième tour et l'avant-dernier tour de chaque groupe : c'est à dire, dans T2, T3 de G1, T6, T7 de G2, T10, T11 de G3 et T14 et T15 de G4.

Les troisièmes moyens  $TC_1$  sont utilisés dans le premier tour et le dernier tour de chaque groupe. C'est à dire dans T1, T4 de G1, T5, T8 de G2, T9, T12 de G3 et T13, T16 de G4.

En pratique, ces différents moyens sont des tables de constantes. les premiers moyens correspondent à la première table de constantes  $TC_0$ , correspondant à l'exécution normale du DES. Les autres moyens  $TC_1$  et  $TC_2$  se définissent par rapport à cette première table de constantes  $TC_0$ , par complémentation.

Les deuxièmes moyens  $TC_2$  sont tels que pour le complément /E de la donnée d'entrée E, ils fournissent le complément de la donnée de sortie S des premiers moyens  $TC_0$ . Un exemple d'une deuxième table élémentaire  $TC_{21}$  correspondant à la première table de constante élémentaire  $TC_{01}$  est représenté sur la figure 9. On notera que la notation du complément /E utilisée dans

le texte, correspond la notation avec une barre au-dessus de la donnée complémentée sur les dessins.

Les troisièmes moyens sont tels que pour la donnée d'entrée E, ils fournissent le complément /S de la donnée de sortie S des premiers moyens  $TC_0$ . Un exemple  
5 d'une troisième table élémentaire  $TC_1$  correspondant à la première table de constante élémentaire  $TC_0$  est représenté sur la figure 10.

Le programme de calcul consiste alors au début de  
10 l'exécution de l'algorithme, à tirer une valeur aléatoire RND1 égale à 0 ou à 1, puis à tester cette valeur RND1. Dans l'exemple, si RND1 vaut 1, on effectue le calcul en utilisant la deuxième séquence SEQB pour chaque groupe G1 à G4.

15 Si RND1 vaut 0, on effectue le calcul en utilisant la première séquence SEQA pour chaque groupe.

Que l'on utilise la première ou la deuxième séquence, on obtient, à la sortie de chaque groupe, le résultat juste pour les paramètres de sortie. Ainsi,  
20 les paramètres de sortie L4 et R4 du premier groupe G1, L8 et R8 du deuxième groupe G2, L12 et R12 du troisième groupe G3, L16 et R16 du quatrième groupe G4 sont justes quelle que soit la séquence utilisée.

Quand on a effectué tous les tours, on obtient les  
25 paramètres justes L16 et R16 qui vont permettre de calculer le message chiffré C juste.

Par contre, à l'intérieur des groupes, certains résultats intermédiaires n'ont pas les mêmes valeurs selon la séquence utilisée, mais des valeurs  
30 complémentaires, comme on va le montrer par référence aux figures 3 et 8.

La figure 3 déjà décrite correspond en fait à l'organigramme de calcul des quatre tours T1, T2, T3 et T4 du premier groupe G1, dans la première séquence  
35 SEQA.

La figure 8 montre l'organigramme détaillé des quatre tours T1, T2, T3 et T4 du premier groupe G1, dans la deuxième séquence SEQB.

5 Dans cette deuxième séquence, le tour T1 utilise les troisièmes moyens  $TC_1$ . En sortie de l'opération SBOX, on obtient donc la donnée /a (Figure 8), au lieu de la donnée a avec la première séquence SEQA (Figure 3).

10 L'opération P PERM du tour T1 qui est une simple permutation va donc également fournir en sortie une donnée complémentée /c par rapport à la séquence SEQA.

La donnée g qui est obtenue par un OU EXCLUSIF entre une donnée complémentée /c et une donnée non complémentée L0, va aussi fournir en sortie une donnée  
15 complémentée /g.

Ainsi, avec les troisièmes moyens du tour T1 on obtient toutes les données complémentées suivantes, par rapport aux données qui seraient obtenues avec la séquence SEQA :

- 20
- dans le tour T1 : /a, /c, /g;
  - dans le tour T2 : /R1, /h, /l, /b;
  - dans le tour T3 : /L2.

On arrive alors aux deuxièmes moyens  $TC_2$  utilisés dans le tour T2. D'après leur définition, en appliquant  
25 la donnée complémentée /b, on obtient en sortie la donnée complémentée /a. En conduisant ce raisonnement jusqu'à la fin du tour T4, en remarquant qu'un OU EXCLUSIF entre deux données complémentées donne un résultat non complémenté (par exemple /L3 XOR /c = g  
30 dans le tour T4), on obtient en sortie du tour T4, les données L4, R4 non complémentées.

En outre, on constate que pour toutes les instructions critiques de début de DES, les instructions critiques vont manipuler, de manière  
35 aléatoire en fonction de la donnée RND1, les données ou

leurs compléments selon que la séquence exécutée est la première SEQA ou la deuxième SEQB.

Le procédé de contre-mesure, dans ce premier mode de réalisation est donc très intéressant. Il ne  
5 nécessite que deux opérations supplémentaires, dans le programme de calcul du DES qui sont le tirage de la valeur aléatoire et le test de cette valeur. La mémoire programme doit, elle, contenir les trois moyens différents utilisés, c'est à dire les trois tables de  
10 constantes  $TC_0$ ,  $TC_1$ ,  $TC_2$ .

En revenant à la figure 7, on pourra noter, que l'on n'a pas besoin de contre-mesure dans les groupes du milieu G2 et G3, puisqu'ils ne contiennent pas d'instructions critiques au sens attaque DPA. On  
15 pourrait donc n'appliquer le procédé de contre-mesure avec ses deux séquences SEQA et SEQB qu'au premier et au dernier groupe G1 et G4. Il suffirait d'appliquer systématiquement la première séquence SEQA aux groupes G2 et G3.

20 Mais le fait de d'appliquer le procédé de contre-mesure à tous les groupes donne une cohérence à l'ensemble.

Ainsi, on associe de préférence les deux séquences SEQA et SEOB à chacun des groupes G1 à G4.

25 Un deuxième mode de réalisation du procédé de contre-mesure selon l'invention est représenté sur la figure 11. Ce deuxième mode de réalisation est en fait une variante du premier. L'intérêt de cette variante est de n'utiliser comme autres moyens dans la séquence  
30 SEQB, que les deuxièmes moyens  $TC_2$ . En effet, on a vu que les différents moyens  $TC_0$ ,  $TC_1$ ,  $TC_2$  correspondent en pratique à des tables de constantes comprenant chacune huit tables de constantes élémentaires, ce qui occupe un espace non négligeable en mémoire programme.

35 Cette variante consiste donc à utiliser uniquement les deuxièmes moyens  $TC_2$  dans la séquence SEQB. Pour

cela, on prévoit dans le programme de calcul des premiers et derniers tours de chaque groupe, une opération supplémentaire CP, pour compléter la donnée d'entrée appliquée aux deuxièmes moyens. Cette

5 opération supplémentaire CP est en pratique un OU exclusif de la donnée d'entrée avec des 1 logiques. Si on se reporte à la figure 12 représentant l'organigramme détaillé de la deuxième séquence SEQB de calcul des quatre tours T1 à T4 du premier groupe G1,

10 il s'agit de compléter la donnée b avant de l'appliquer en entrée de l'opération SBOX des tours T1 et T4. Comme les deuxièmes moyens  $TC_2$  complètent l'entrée, l'opération de complémentation CP plus les deuxièmes moyens  $TC_2$  équivalent aux troisièmes moyens

15  $TC_1$  utilisés dans le premier mode de réalisation de l'invention, c'est à dire à une donnée non complémentée en entrée.

Mais pour que le procédé de contre-mesure selon ce deuxième mode de réalisation soit efficace, il faut que

20 le nombre d'instructions soit exactement le même quel que soit la séquence de calcul utilisée. En effet si une différence quelconque existait entre les deux séquences SEQA et SEQB possibles, il y aurait alors une possibilité d'attaque DPA fructueuse.

25 Pour cette raison et comme représenté sur la figure 13, on prévoit dans les tours T1 et T4 de la première séquence SEQA, une opération ID de recopie à l'identique, qui consiste en un OU exclusif avec des 0 logiques en entrée de l'opération SBOX, pour ne pas

30 modifier la donnée d'entrée tout en appliquant les mêmes instructions que pour l'opération supplémentaire CP.

De cette manière, on a le même nombre d'instructions dans les deux séquences.

La figure 14 représente un troisième mode de réalisation du procédé de contre-mesure selon l'invention.

Dans ce mode de réalisation, on forme un premier  
5 groupe G1 avec les trois premiers tours T1, T2, T3 et  
un autre groupe G4 avec les trois derniers tours T14,  
T15, T16. On associe à chaque groupe une première  
séquence SEQA utilisant les premiers moyens  $TC_0$  pour  
chaque tour et une deuxième séquence utilisant d'autres  
10 moyens pour certains tours au moins.

En sortie de chaque groupe G1, G4, on obtient le  
bon résultat en sortie L3, R3 et L16, R16, quelle que  
soit la séquence SEQA ou SEQB utilisée.

Les autres moyens sont dans l'exemple les  
15 troisièmes moyens  $TC_1$  déjà vus en relation avec le  
premier mode de réalisation et des quatrièmes moyens  
 $TC_3$ .

Ces quatrièmes moyens  $TC_3$  sont définis par rapport  
aux premiers moyens  $TC_0$ , comme faisant correspondre la  
20 donnée S de sortie, au complément /E de la donnée E  
d'entrée. Une table de constantes élémentaire  $TC_{31}$   
correspondante est représentée sur la figure 16.

Pour les autres tours non compris dans les groupes,  
c'est à dire pour les tours T4 à T13, on applique les  
25 premiers moyens  $TC_0$ .

Ainsi, après avoir tiré la valeur aléatoire RND1,  
on teste cette valeur pour déterminer la séquence à  
appliquer au premier groupe, on continue en sortie avec  
les paramètres L3, R3 calculés, en exécutant les tours  
30 suivants avec les premiers moyens  $TC_0$ . En fin de tour  
T13, on applique la séquence déterminée par la valeur  
aléatoire RND1 au groupe G4. On obtient les paramètres  
L16, R16 qui vont servir à calculer le message chiffré  
C.

35 La figure 15 est un organigramme détaillé  
correspondant, pour la deuxième séquence SEQB.

L16, R16 qui vont servir à calculer le message chiffré C.

La figure 15 est un organigramme détaillé correspondant, pour la deuxième séquence SEQB.

5 Il apparaît clairement sur cet organigramme que l'on obtient des données complémentées (la complémentation étant notée par une barre au-dessus de la donnée) pour toutes les instructions critiques de ces tours. Et les données L3 et R3 en sortie du  
10 troisième tour ne sont pas complémentées. On peut continuer l'exécution de l'algorithme, en passant au tour T4 auquel on applique les premiers moyens  $TC_0$  selon l'exécution normale de l'algorithme.

15 Sur cette figure, on peut remarquer que dans l'opération SBOX du troisième tour T3, on pourrait utiliser les premiers moyens  $TC_0$  à la place des troisièmes moyens  $TC_1$ , en prévoyant une opération supplémentaire de complémentation CP en sortie de l'opération SBOX. C'est une solution équivalente.

20 Il faut alors faire correspondre à cette opération supplémentaire de complémentation dans la séquence SEQB, l'opération supplémentaire de recopie à l'identique ID dans la séquence SEQA.

25 La figure 17 représente un organigramme d'exécution utilisant cette variante. Pour le troisième tour des deux groupes G1 et G4, on utilise dans la première séquence SEQA, les premiers moyens  $TC_0$  suivis en sortie de l'opération supplémentaire ID de recopie, ce qui est noté  $T3(TC_0, ID)$ . Dans la deuxième séquence SEQB, on  
30 utilise pour le troisième tour les premiers moyens  $TC_0$  suivis en sortie de l'opération supplémentaire de complémentation CP ce qui est noté  $T3(TC_0, CP)$ .

35 Ainsi, le deuxième mode de réalisation et cette variante du troisième mode de réalisation montrent l'utilisation d'opérations supplémentaires en entrée ou en sortie des différents moyens.

entrée ou en sortie des moyens utilisés. A chaque opération supplémentaire de complémentation CP dans la deuxième séquence correspond alors une opération supplémentaire de recopie à l'identique ID dans la première séquence SEQA.

La présente invention s'applique à l'algorithme de cryptographie à clé secrète DES, pour lequel plusieurs exemples d'application non limitatifs ont été décrits. Il s'applique plus généralement dans un algorithme de cryptographie à clé secrète à seize tours de calculs, dont les instructions critiques se situent parmi les instructions des trois premiers ou trois derniers tours.

Un composant électronique 1 mettant en oeuvre un procédé de contre-mesure selon l'invention dans un algorithme de cryptographie à clé secrète DES, comprend typiquement, comme représenté sur la figure 18, un microprocesseur  $\mu P$ , une mémoire programme 2 et une mémoire de travail 3. Pour pouvoir gérer l'utilisation des différents moyens  $TC_0$ ,  $TC_1$ ,  $TC_2$  selon l'invention, qui sont, en pratique, des tables de constantes mémorisées en mémoire programme, des moyens 4 de génération d'une valeur aléatoire entre 0 et 1, sont prévus qui, si on se reporte aux organigrammes des figures 7 et 11, fourniront la valeur de RND1 à chaque exécution du DES. Un tel composant peut tout particulièrement être utilisé dans une carte à puce 5, pour améliorer leur inviolabilité.

## REVENDICATIONS

1. Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (K) pour calculer un message chiffré (C) à partir d'un message d'entrée (M),  
5 la mise en oeuvre de l'algorithme comprenant seize tours de calcul (T1, ..., T16), chaque tour utilisant des premiers moyens (TC<sub>0</sub>) pour fournir une donnée de sortie à partir d'une donnée d'entrée, la donnée de sortie et/ou des données dérivées étant manipulées par  
10 des instructions critiques dans les trois premiers (T1, T2, T3) et les trois derniers tours (T14, T15, T16), caractérisé en ce que l'on forme un groupe (G1) comprenant les trois premiers tours au moins et un autre groupe (G4) comprenant les trois derniers tours  
15 au moins, et en ce que l'on associe à chacun de ces groupes (G1 et G4) une première séquence (SEQA) utilisant les premiers moyens (TC<sub>0</sub>) dans chaque tour et une deuxième séquence (SEQB) utilisant d'autres moyens (TC<sub>1</sub>, TC<sub>2</sub>, TC<sub>3</sub>) dans certains tours au moins, les dites  
20 première et deuxième séquences étant telles qu'elles fournissent un même résultat en sortie du dernier tour de chaque groupe pour un même message d'entrée (M) donné, le choix de la séquence à exécuter dans les groupes concernés étant fonction d'une loi statistique  
25 de probabilité un demi, pour rendre imprédictibles toutes les données manipulées par les dites instructions critiques.

2. Procédé de contre-mesure selon la revendication  
30 1, caractérisé en ce que les autres moyens sont tels qu'ils complémentent l'une et/ou l'autre des données d'entrée (E) et/ou de sortie (S) des premiers moyens.

3. Procédé de contre-mesure selon la revendication 2, caractérisé en ce que la deuxième séquence (SEQB) comprend pour un ou plusieurs tours une opération supplémentaire de complémentation (CP) en entrée ou en sortie des moyens utilisés, et en ce qu'à chaque opération supplémentaire de complémentation dans la deuxième séquence correspond une opération supplémentaire de recopie à l'identique (ID) dans la première séquence (SEQA).

4. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que l'on forme quatre groupes (G1,...G4) de quatre tours successifs chacun (T1,...T4), en ce que l'on associe à chaque groupe la première séquence (SEQA) et en ce que l'on associe au moins au premier groupe (G1) et au dernier groupe (G4) la deuxième séquence (SEQB).

5. Procédé de contre-mesure selon la revendication 4, caractérisé en ce que la deuxième séquence (SEQB) est associée à chacun des groupes (G1,...G4).

6. Procédé de contre-mesure selon l'une quelconque des revendications 1 à 3, caractérisé en ce que le premier groupe (G1) est formé des trois premiers tours (T1, T2, T3) et en ce que le dernier groupe est formé des trois derniers tours (T14, T15, T16).

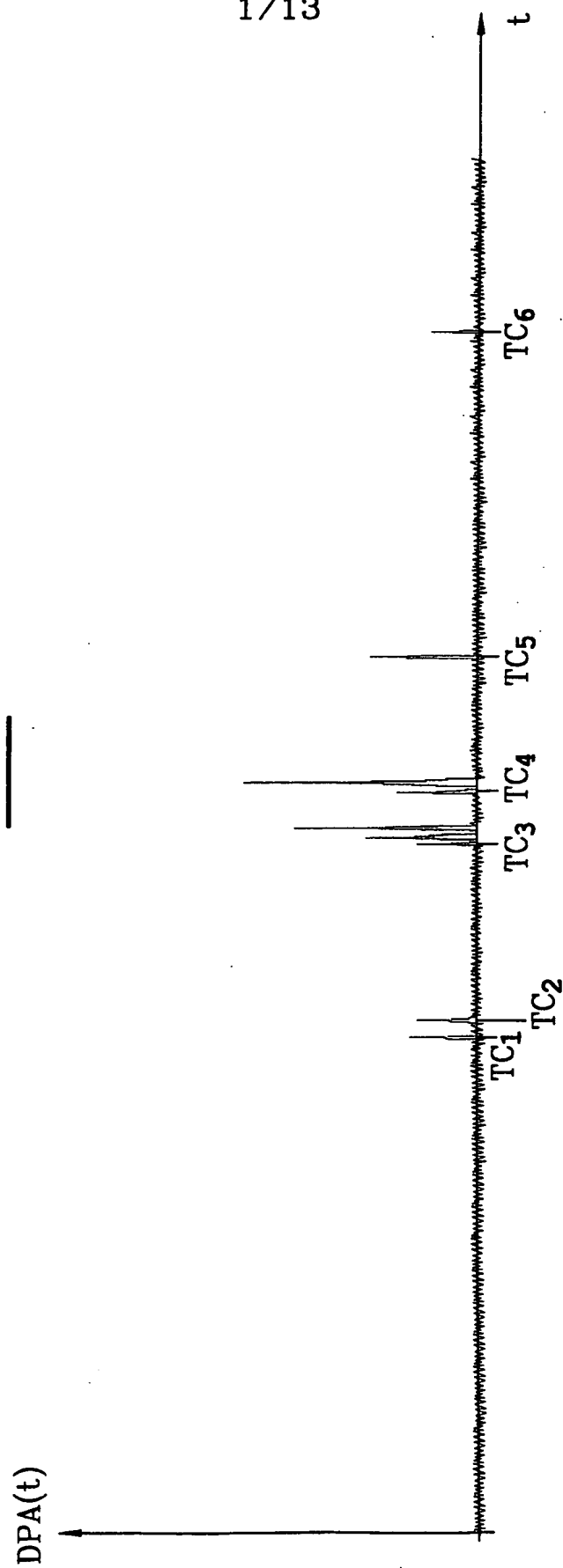
7. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que le choix de la séquence à exécuter se fait au début de l'exécution de l'algorithme par tirage d'une valeur aléatoire (RND1), la séquence choisie étant celle utilisée dans chacun des groupes concernés.

8. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens sont des tables de constantes.

5           9. Composant électronique de sécurité mettant en oeuvre le procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens ( $TC_0$ ,  $TC_1$ ,  $TC_2$ ) pour  
10 fournir une donnée de sortie à partir d'une donnée d'entrée sont fixés en mémoire programme du dit composant et en ce qu'il comprend des moyens (4) de génération d'une valeur aléatoire (RND1) à 0 ou à 1 pour gérer l'utilisation des dits différents moyens.

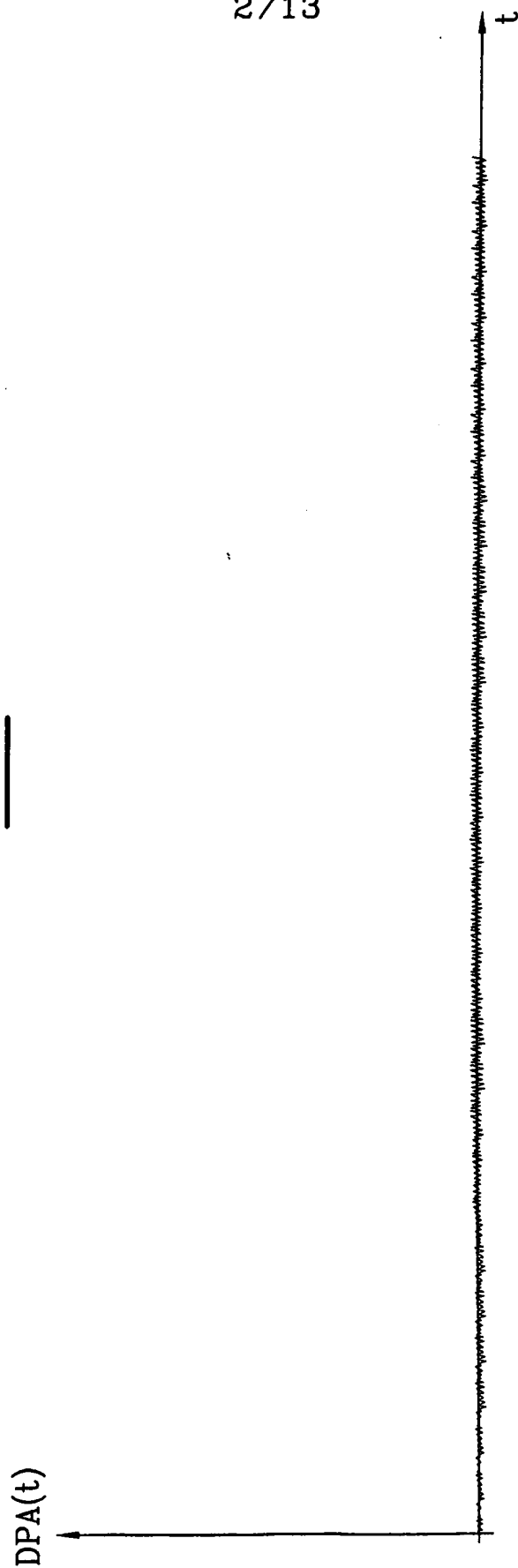
15           10. Carte à puce comprenant un composant électronique de sécurité selon la revendication 9.

1/13

**FIG.1**

2/13

FIG.2



3/13

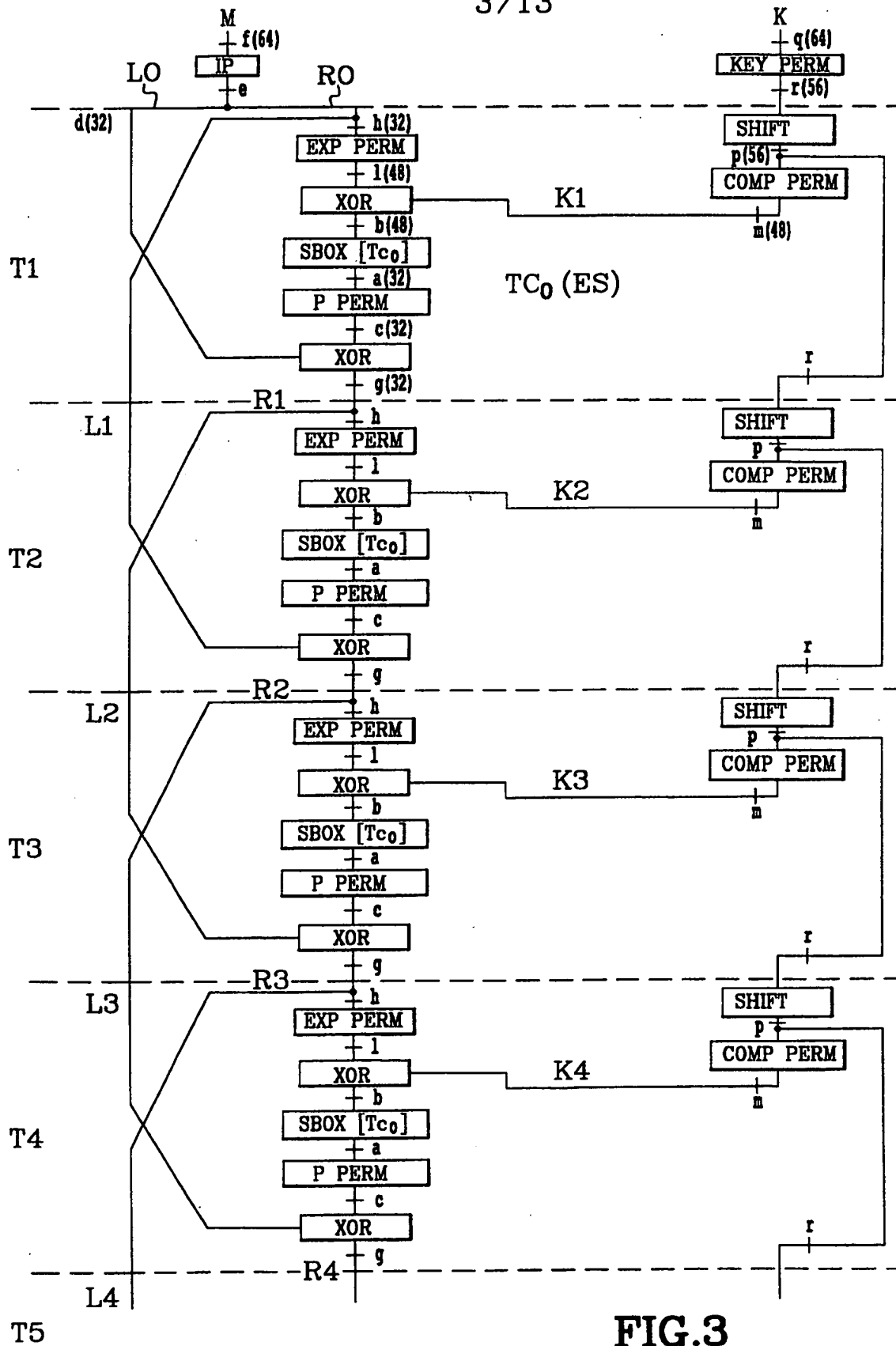


FIG.3

4/13

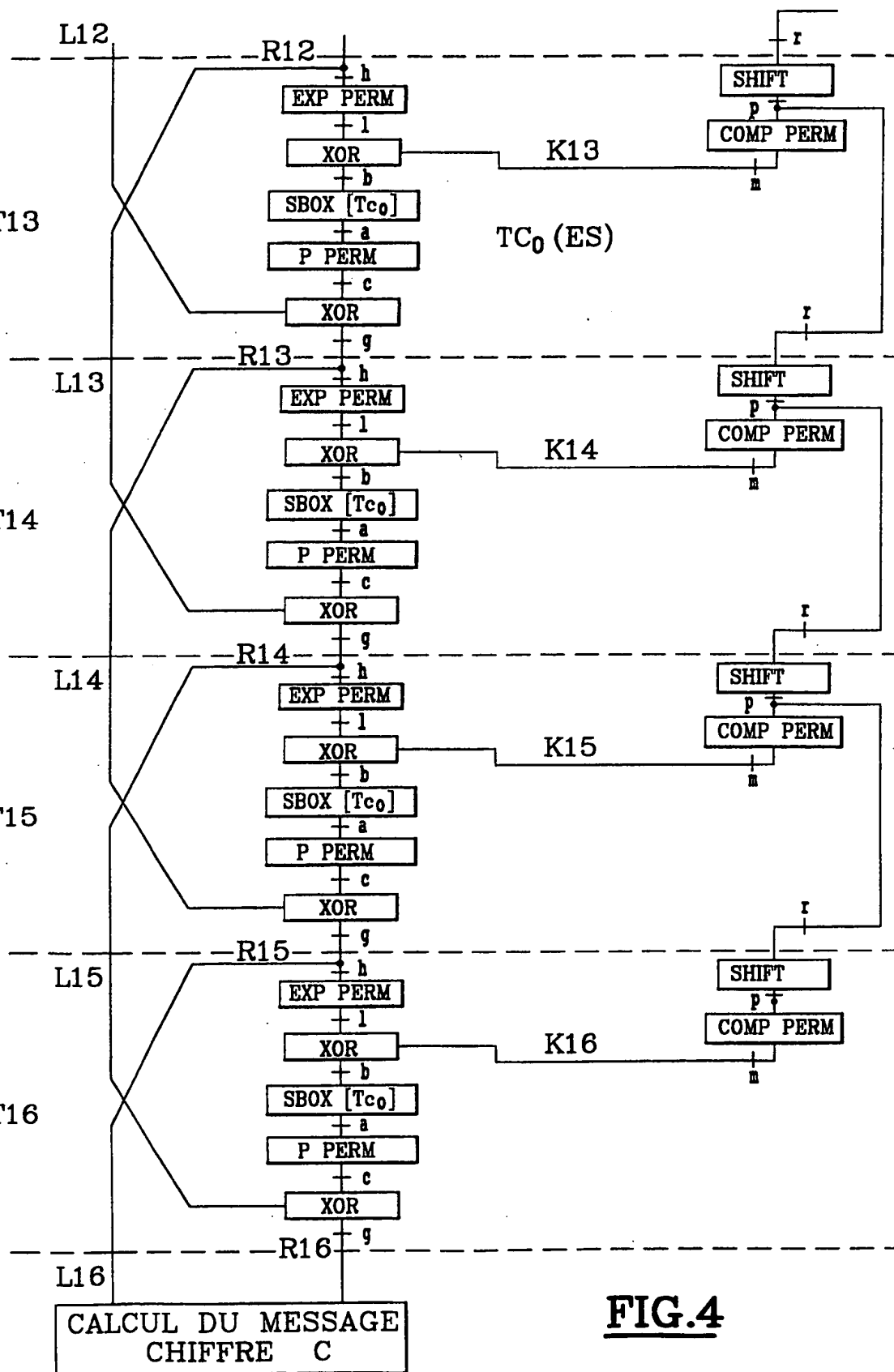
T12

T13

T14

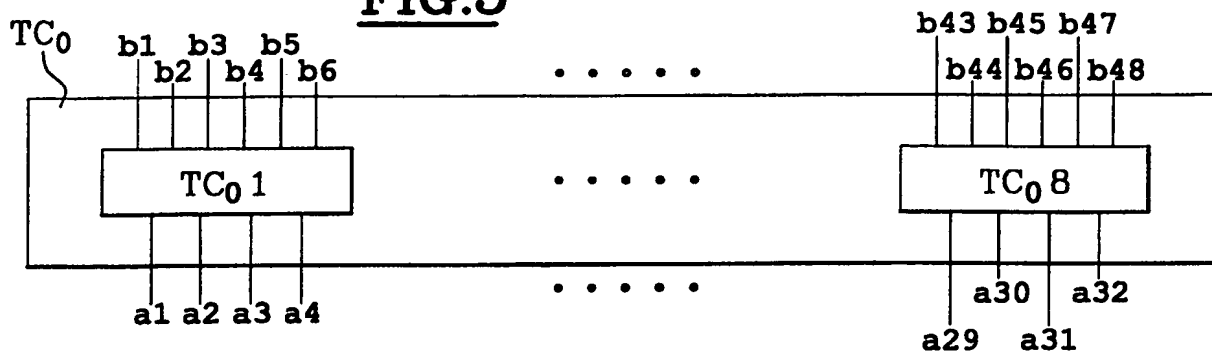
T15

T16

**FIG.4**

5/13

**FIG.5**



**FIG.6**

TC<sub>0</sub> 1

E=b1b2b3b4b5b6	S=a1a2a3a4
000000	1101
000001	0101
⋮	⋮
111111	1010

**FIG.10**

TC<sub>1</sub> 1

E=b1b2b3b4b5b6	/S=a1a2a3a4
000000	0010
000001	1010
⋮	⋮
111111	0101

**FIG.9**

TC<sub>2</sub> 1

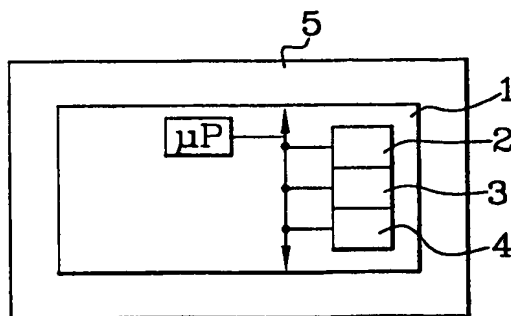
/E=b1b2b3b4b5b6	/S=a1a2a3a4
000000	0101
⋮	⋮
111110	1010
111111	0010

**FIG.16**

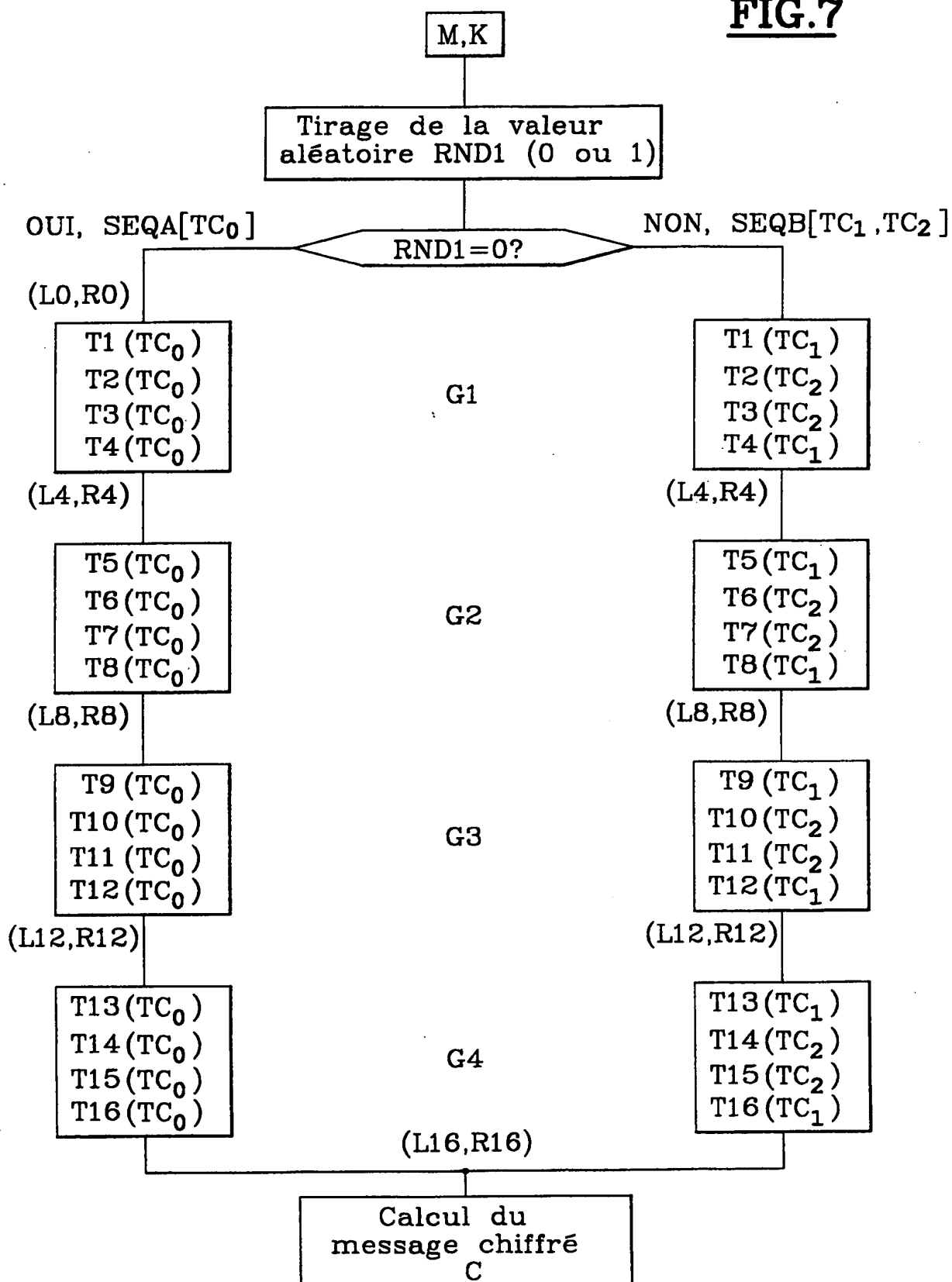
TC<sub>3</sub> 1

/E=b1b2b3b4b5b6	S=a1a2a3a4
000000	1010
⋮	⋮
111110	0101
111111	1101

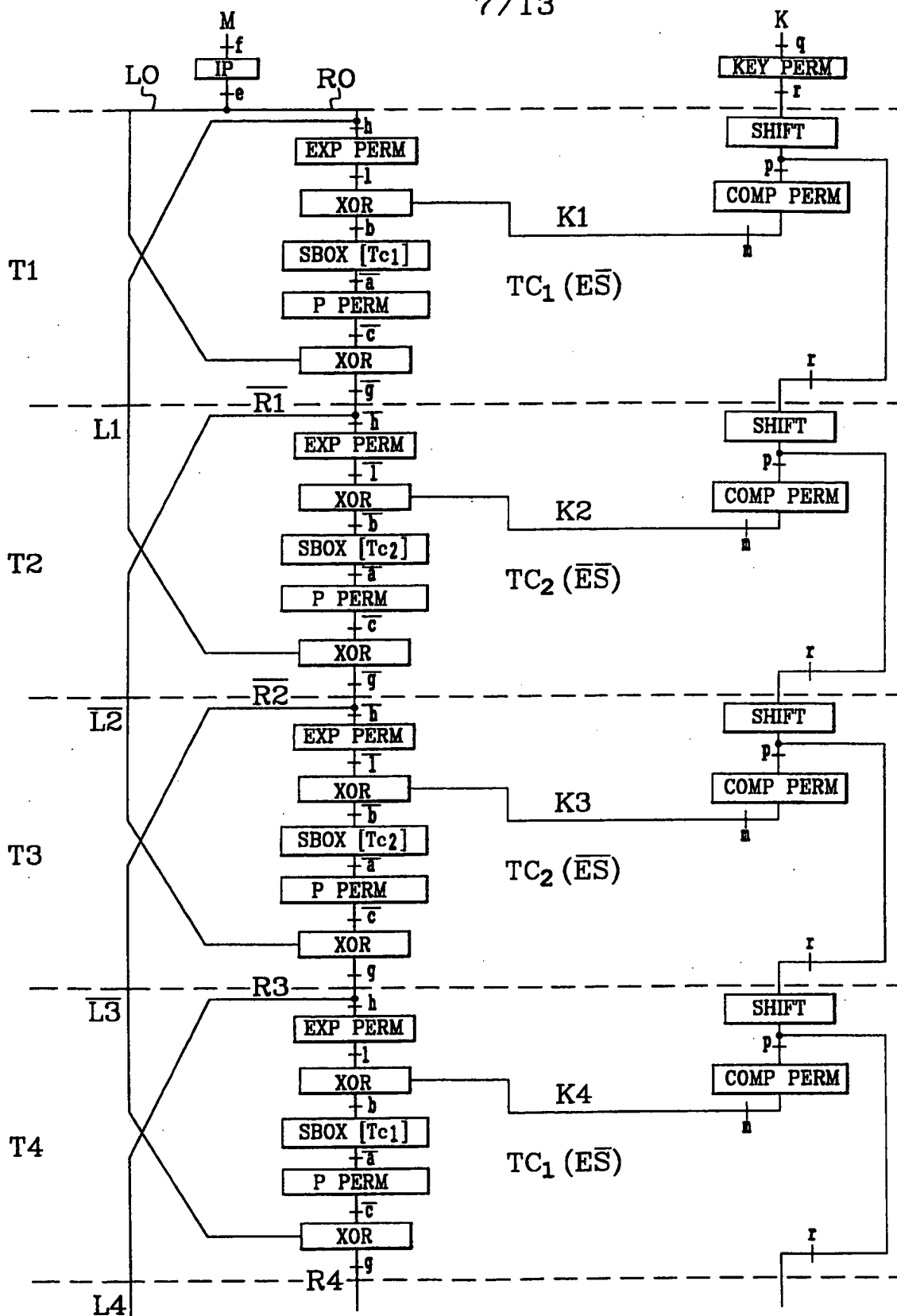
**FIG.18**



6/13

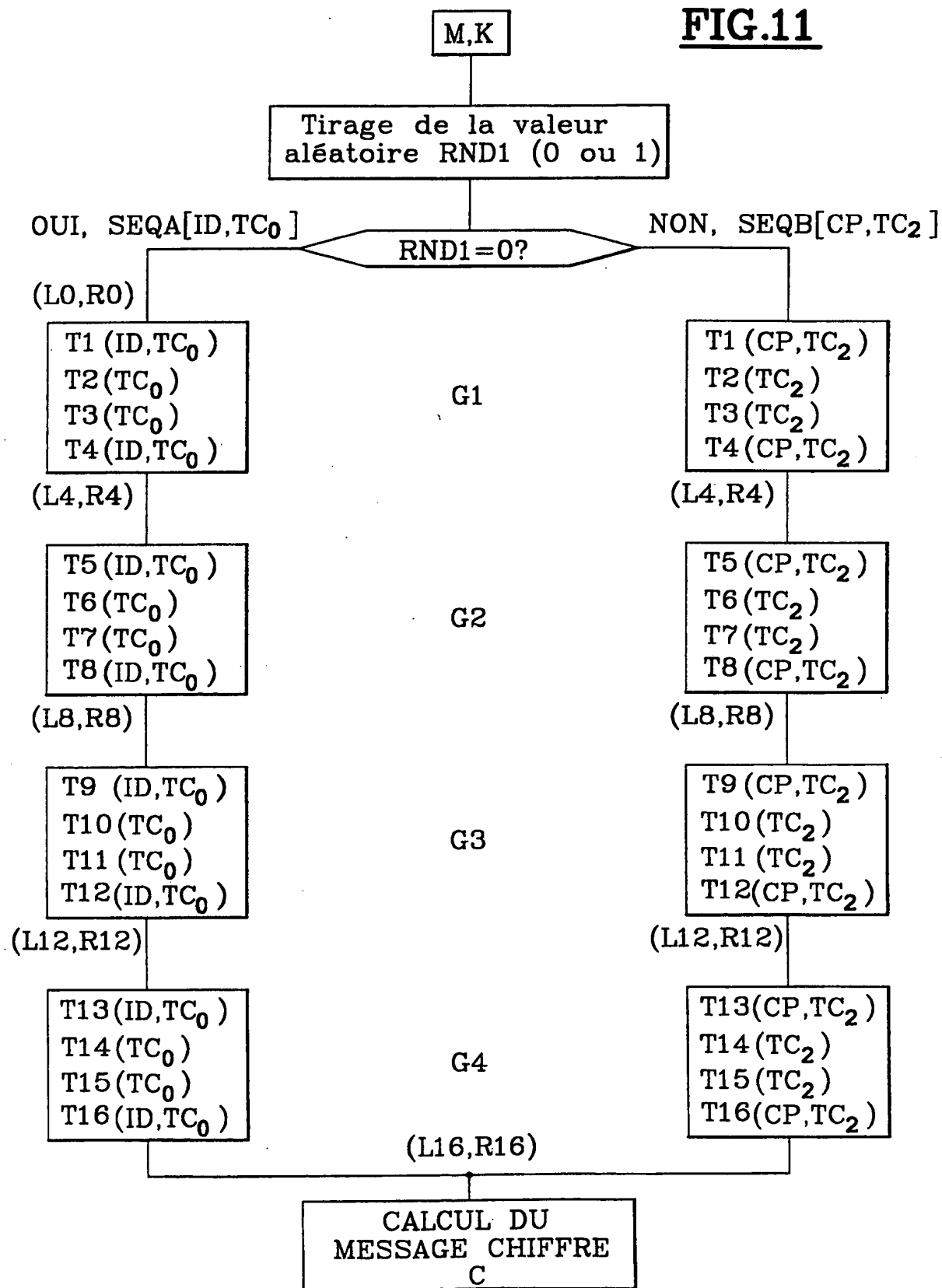
**FIG.7**

7/13

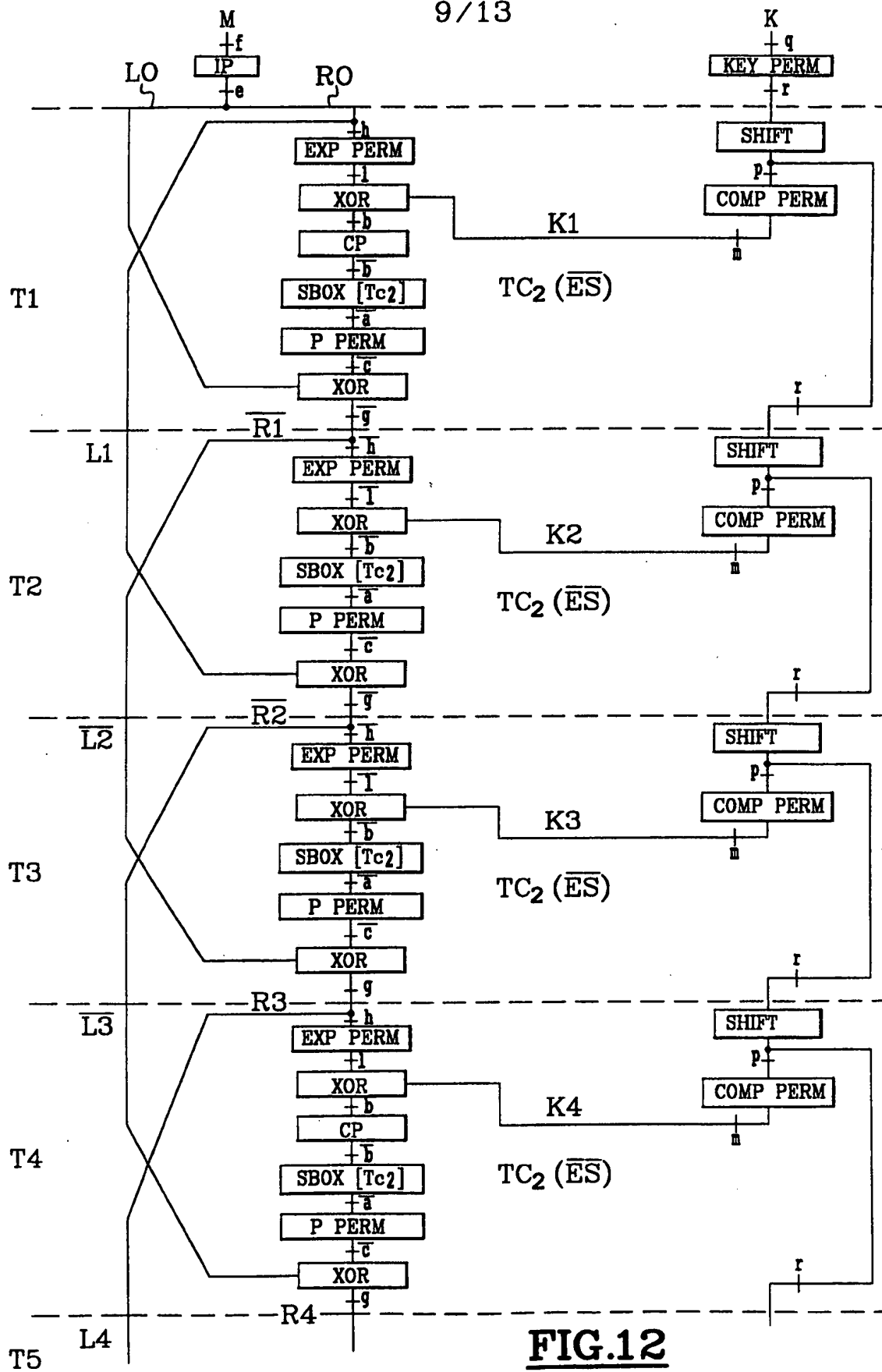


**FIG.8**

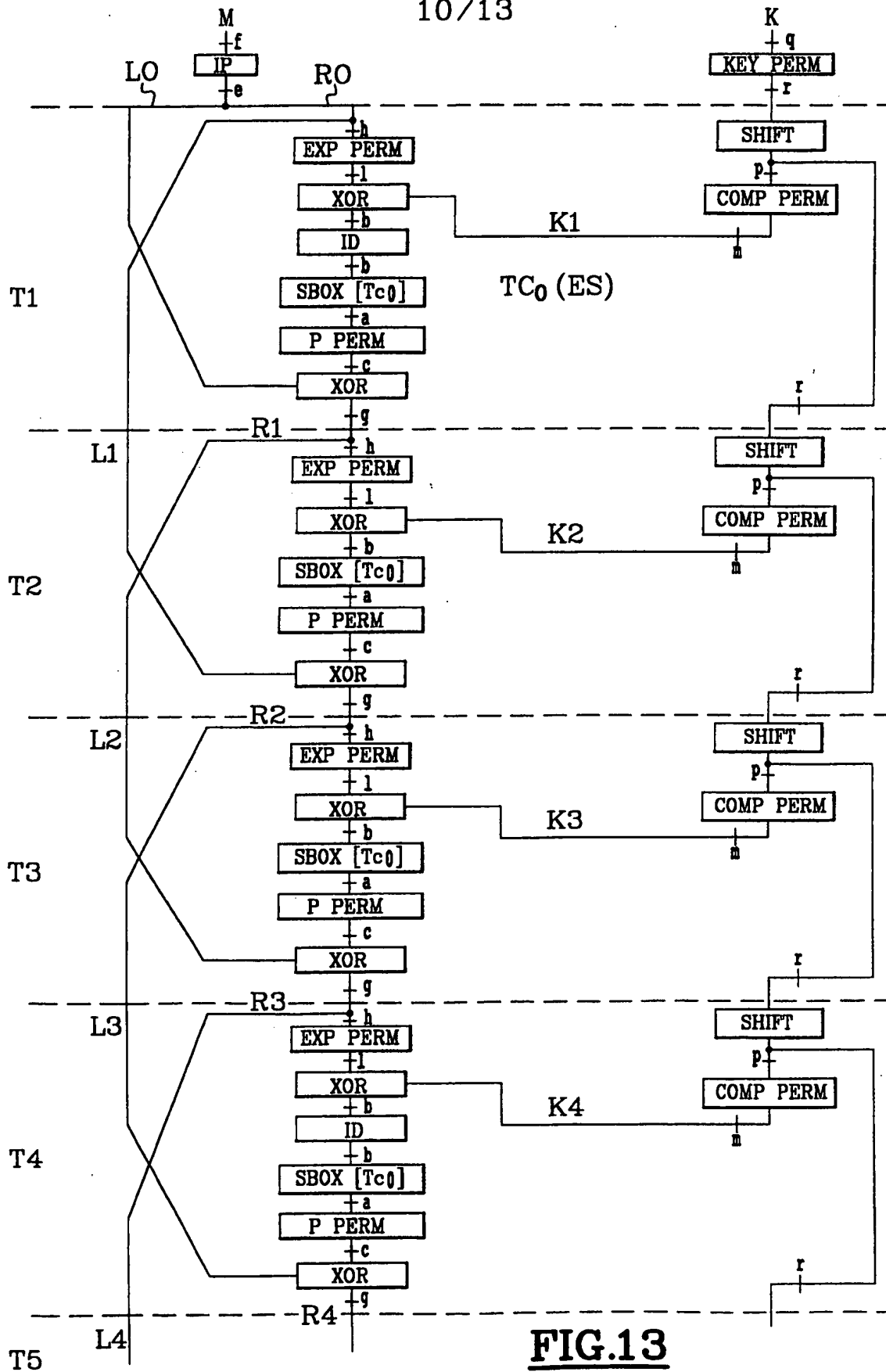
8/13

**FIG.11**

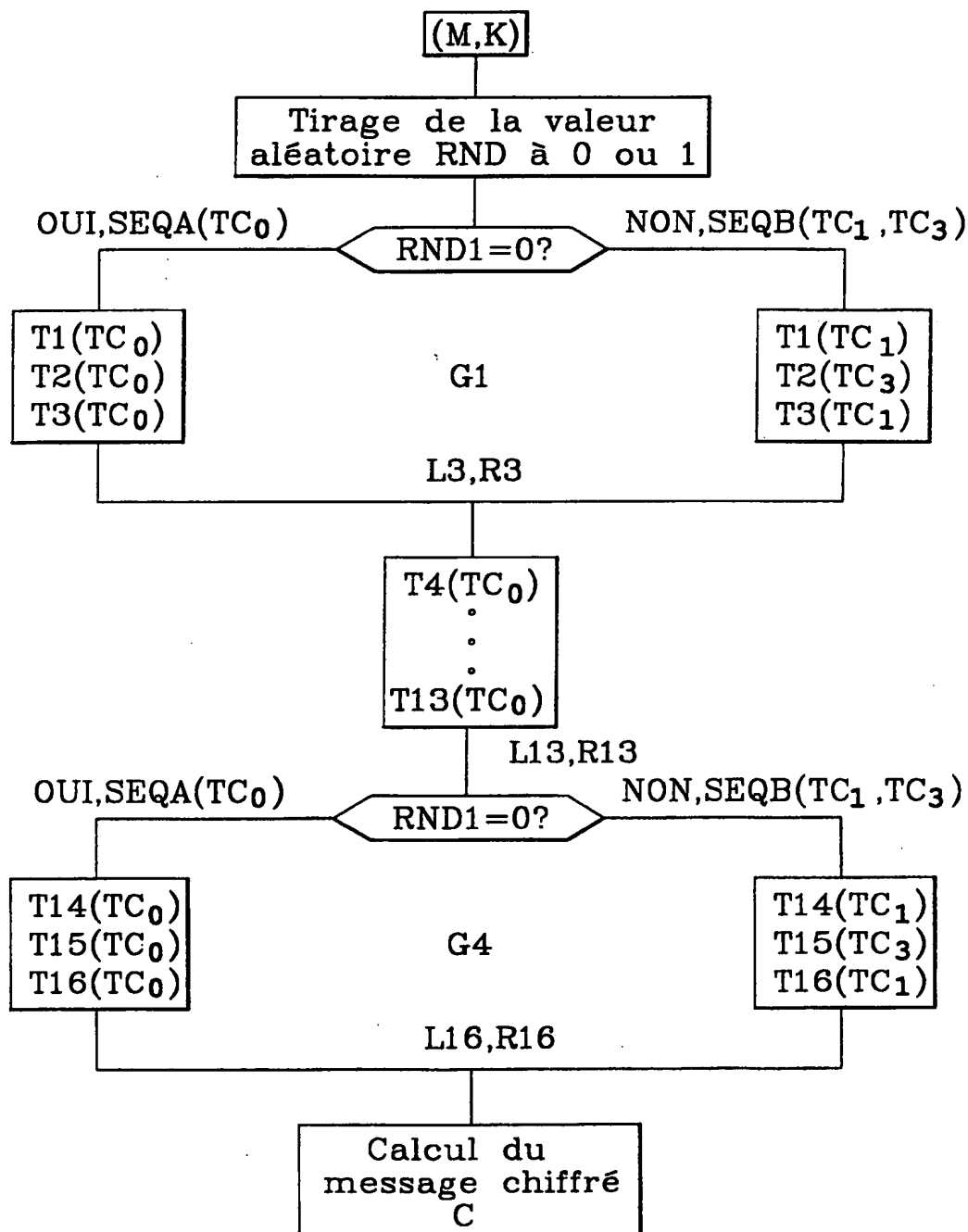
9/13



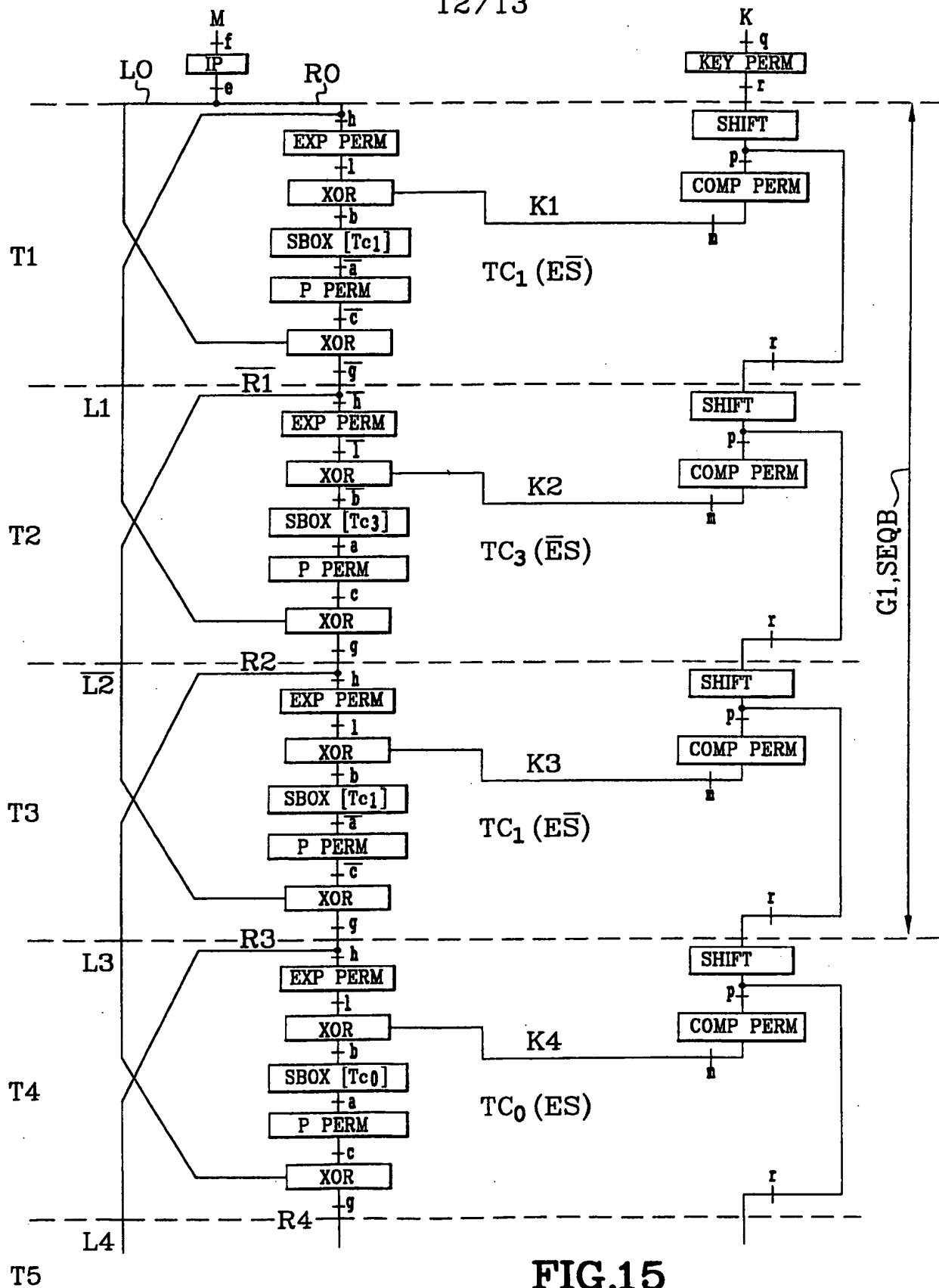
10/13



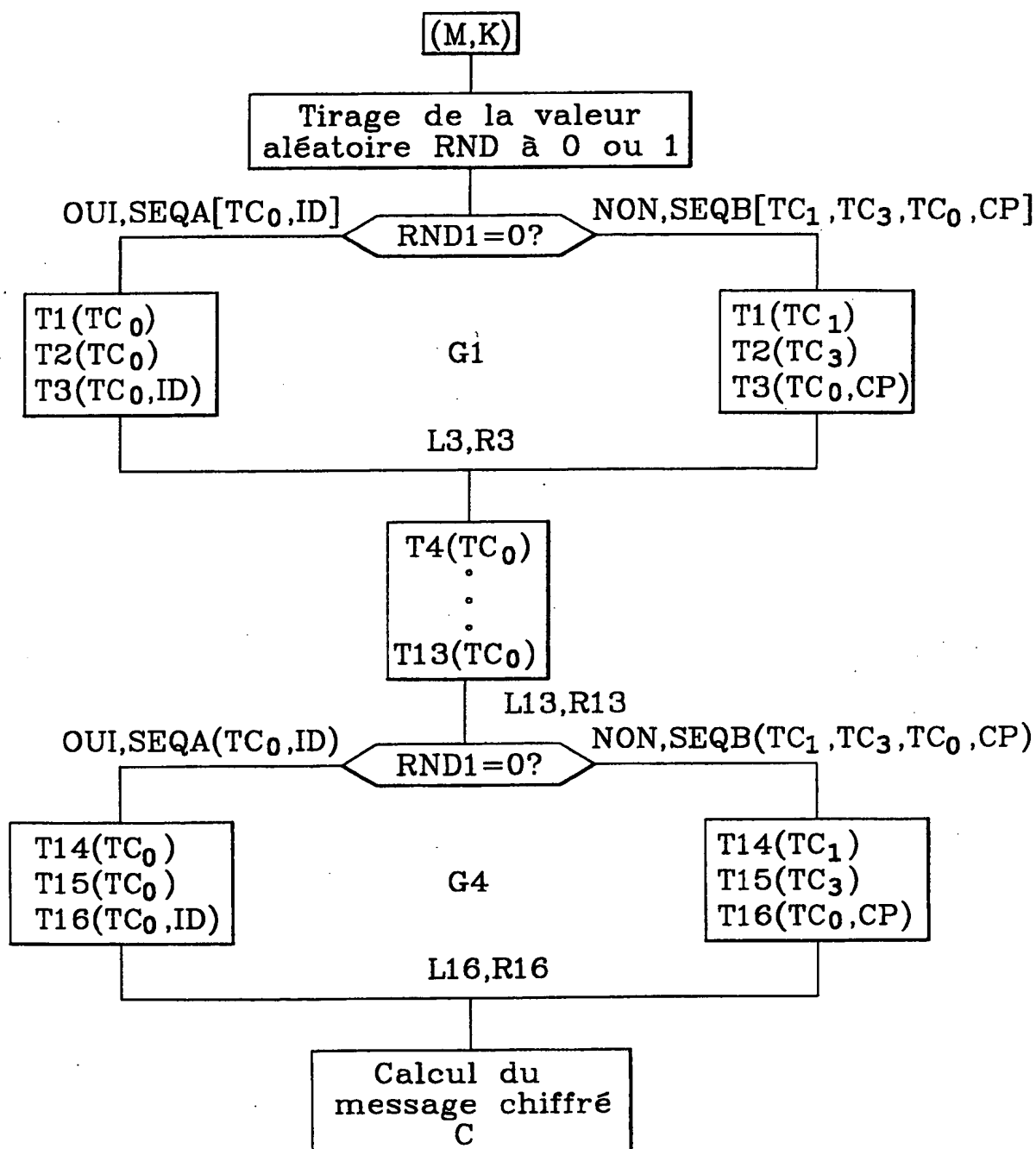
11/13

**FIG.14**

12/13

**FIG.15**

13/13

**FIG.17**

# INTERNATIONAL SEARCH REPORT

Inter: nal Application No

PCT/FR 99/02199

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 November 1997 (1997-11-03), pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS abstract column 1, line 13 - line 29 column 2, line 6 - line 18 column 3, line 1 -column 5, line 1 --- -/--</p>	1,2,4

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

10 January 2000

Date of mailing of the international search report

18/01/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Gautier, L

# INTERNATIONAL SEARCH REPORT

Inter.      nal Application No

PCT/FR 99/02199

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THECONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 July 1994 (1994-07-01), pages 85-90, XP000460342 the whole document</p> <p style="text-align: center;">---</p>	1
A	<p>FR 2 672 402 A (GEMPLUS CARD INT) 7 August 1992 (1992-08-07) abstract page 1, line 4 - line 12 page 3, line 19 - line 23 figure 1 claim 1</p> <p style="text-align: center;">-----</p>	9,10

# INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/FR 99/02199

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2672402    A	07-08-1992	NONE	

# RAPPORT DE RECHERCHE INTERNATIONALE

Den 3 Internationale No

PCT/FR 99/02199

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

## C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997 (1997-11-03), pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS abrégé colonne 1, ligne 13 - ligne 29 colonne 2, ligne 6 - ligne 18 colonne 3, ligne 1 - colonne 5, ligne 1 --- -/--</p>	1, 2, 4

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

10 janvier 2000

Date d'expédition du présent rapport de recherche internationale

18/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Gautier, L

# RAPPORT DE RECHERCHE INTERNATIONALE

Dem. Internationale No

PCT/FR 99/02199

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités. avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 juillet 1994 (1994-07-01), pages 85-90, XP000460342 le document en entier ---</p>	1
A	<p>FR 2 672 402 A (GEMPLUS CARD INT) 7 août 1992 (1992-08-07) abrégé page 1, ligne 4 - ligne 12 page 3, ligne 19 - ligne 23 figure 1 revendication 1 -----</p>	9,10

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. Internationale No

PCT/FR 99/02199

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2672402      A	07-08-1992	AUCUN	